

Threat Trees, Platform Trees, and Their Connection
William Jackson, Daniel Hicks, and Jack Reed
US Army RDECOM
Warren, Michigan

ABSTRACT

The Threat Oriented Survivability Optimization Model (TOSOM), [1], is a simple, first-order model used to evaluate the worth of suites of countermeasures in protecting a combat platform.

In a typical TOSOM study, one of the first steps is to develop the threats that the platform in question will encounter. These threats are arranged in threat tree form; that is, the threats are broken into classes of threats (for example, Direct Fire, Indirect Fire, Air), and then each class is divided into a subclass; this process continues until the actual threats encountered by the platform in question are enumerated. Each branch of the tree is also given a relative probability of occurrence (that is, the sum of the probabilities of all branches emanating from each node of the tree must be equal to 1). Thus, ignoring the special tree structure arrangement of the threats, a threat tree is in essence the distribution of threats attacking a single platform.

In a system-of-systems environment each platform will possess its own threat tree. Also of interest in such an environment is what will be called a platform tree; that is, the distribution of platforms that are attacked by a single type of threat.

In this paper we wish to examine threat trees, platform trees, their connection, and how they might be combined in order to provide a comprehensive view of the battlefield threat situation encountered by a system-of-systems.

INTRODUCTION

The purpose of the model TOSOM is to select a suite of countermeasures, constrained by cost, weight, and other burdens, that will maximize the survivability of a particular type of platform, subject to the given constraints. Historically, it was accepted that to maximize the survivability of the force, it was sufficient to maximize the survivability of each type of combat platform. For this task TOSOM has proven its worth. However, in a system-of-systems environment, while it is true that near maximum force survivability can be obtained by maximizing the survivability of the individual platforms comprising that force, it also may be the case that this level of survivability can be achieved in a more effective fashion. What information is needed to investigate this possibility? Is knowledge of each platform's threat tree sufficient? Thus, the question that motivates this paper is one first asked by Frederick Schwarz, [2], namely: How can threat trees for various platforms be combined into a threat tree for the force? The rough answer, developed below, is that they can't. That is, though threat trees for the individual

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 21 JUL 2004		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Threat Trees, Platform Trees, and Their Connection				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Jackson, William; Hicks, Daniel; Reed, Jack				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USA TACOM 6501 E 11 Mile Road Warren, MI 48397-5000				8. PERFORMING ORGANIZATION REPORT NUMBER 14182	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S) TACOM TARDEC	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 10	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

platforms are sufficient to maximize each platform's survivability, they are collectively insufficient to describe the entire battlefield environment.

If threat trees can't be combined to yield the force structure for a system-of-systems, then could platform trees be so combined? Again, the rough answer is that they cannot. There are other questions that are of relevance here. For example, what is the connection between threat trees and platform trees? Does either type of tree determine the other? And if neither threat trees nor platform trees provide an adequate description of the system-of-systems' threat environment, what information would be required for such a description?

DEFINITIONS AND EXAMPLES

Ultimately, a *threat tree* is a list of threats against a particular platform that are judged to be available to an enemy for use against that platform and associated with each threat in the list is a probability of encounter, with the condition that the sum of the probabilities of encounter for all threats on the list be equal to 1.

In Figure 1 an example of a very simple threat tree is presented.

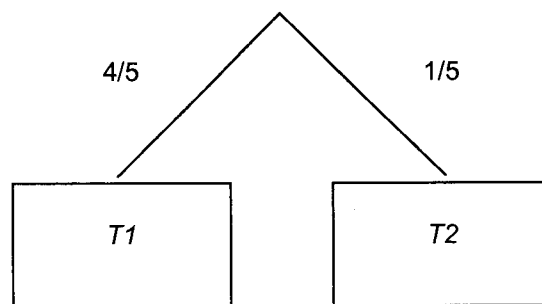


Figure 1. A simple threat tree.

A non-graphical representation of the threat tree shown in Figure 1 is given by: $\{T1, .8; T2, .2\}$.

Figure 2 provides an example of a more realistic and typical threat tree.

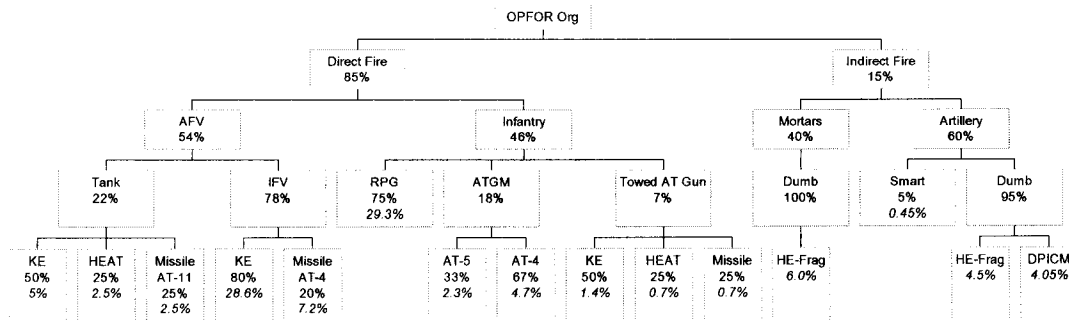


Figure 2. A typical threat tree.

A non-graphical representation of this threat tree is given by: {Threat 1, .04;}, where each probability of encounter is calculated by multiply down the braches of the tree. For example, the probability of encounter for Threat 1 is calculated as follows: $a \times b \times c \times d$ which gives .04.

A *platform tree* is a list of platforms attackable by a particular threat together with a probability of engagement for each platform, with the condition that the sum of the probabilities of engagement for all platforms on the list be equal to 1.

Figure 3 provides an example of a simple platform tree. When viewing the platform tree, recall that a single (type) of threat is understood.

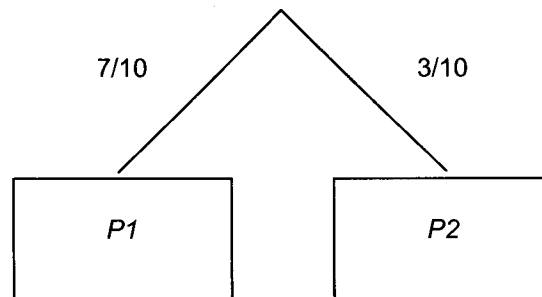


Figure 3. A simple platform tree.

The platform tree in Figure 3 means that an enemy will engage *P1*-type platforms with 70% of his stock of the given threat, and will engage *P2*-type platforms with the remaining 30% of the postulated threat.

A non-graphical representation of the platform tree given in Figure 3 is: {*P1*, .7; *P2*, .3}.

A more typical and more realistic platform tree is shown in Figure 4.

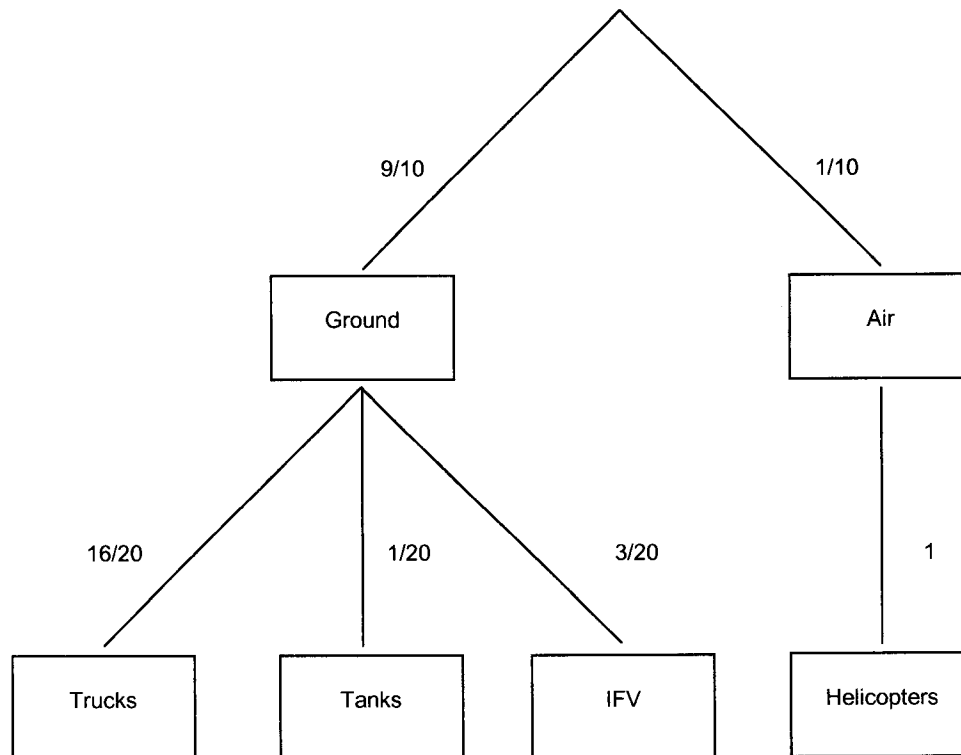


Figure 4. A typical platform tree.

The understood threat in Figure 4 is a rocket propelled grenade (RPG). For the platform tree illustrated in Figure 4 a non-graphical representation is: {Truck, .720; Tank, .045; IFV, .135; Helicopter, .100}, or, more descriptively if the understood threat needs explicit emphasis, {RPG- Truck, .720; Tank, .045; IFV, .135; Helicopter, .100}, where the probabilities of engagement are obtained by multiplying down the branches of the tree.

COMBINING SCENARIOS

Consider the situation in which the particular platform under study is to be used in two different scenarios, for example, a major combat operation and an insurgency. Suppose further that the threat trees for these two operations are as given in Figure 5.

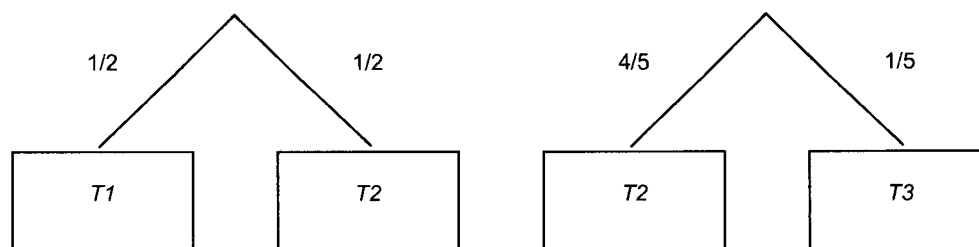


Figure 5. Threat trees, same platform, different scenarios.

In designing a countermeasure suite for the platform under consideration, the analyst has at least two choices. First, he could design a countermeasure suite for each scenario. This approach has the advantage of optimizing the survivability of the platform in each scenario, but has the disadvantage of essentially creating two platforms with the attendant double impact upon logistical and training considerations.

A second approach is to estimate the frequency with which each scenario is expected to occur, and then to create a single composite threat tree. For example, suppose that the first scenario, the major combat operation, is expected to occur only 20% of the time, while insurgencies are expected to occur the remaining 80% of the time. Then a composite tree for the platform and scenarios under study would be that presented in Figure 6, which would collapse to the threat tree given in Figure 7.

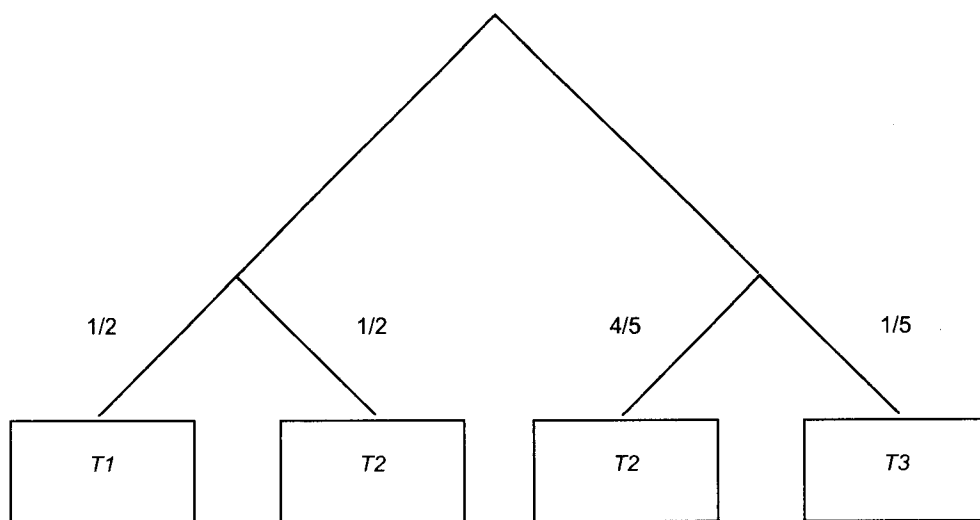


Figure 6. Composite threat tree.

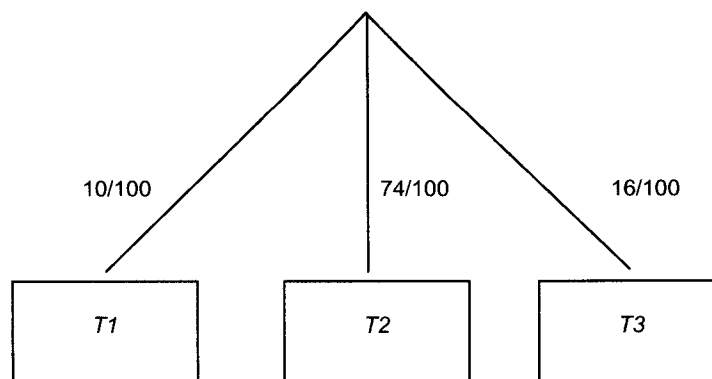


Figure 7. Composite threat tree collapsed.

Using a composite threat tree to design a countermeasure suite for a platform has the disadvantage that the platform is not optimized for either scenario, though with care in selecting the countermeasure suite it will perform better than the baseline in each of the scenarios. This approach works especially well if there is considerable overlap in the threats common to the pair of scenarios. The advantage of this approach is that a single platform is created with its attendant easing of training and logistical issues.

Generally, in selecting a countermeasure suite to enhance the protection of a platform the analyst considers only threat trees for the platform under consideration; he justifiably ignores platform trees. Nevertheless, platform trees for different scenarios can be usefully combined in a fashion analogous to that used for combining threat trees.

As noted above, threat trees for the same platform in different scenarios can be combined in a fashion that the analyst can use, and similarly with platform trees. However, in a system-of-systems environment, it's desired to fix the scenario (at least initially) and to combine threat trees for distinct platforms and platform trees for distinct threats into something that the analyst can use in improving the survivability of the entire force.

The goal then is to determine what information is required in order that the given scenario be determined. By this is meant enough information that all the threat trees and platform trees are determined.

For ease of illustration, the simplest scenario with multiple threats and multiple platforms will be assumed, that is, it will be assumed that there are just two threats, $T1$ and $T2$, and two platforms, $P1$ and $P2$.

PLATFORM TREES ARE NOT DETERMINED BY THREAT TREES

To demonstrate that platform trees are not determined by threat trees it is sufficient to construct a pair of threat trees that are consistent with two distinct pairs of platform trees. To this end consider the threat trees given in Figure 8.

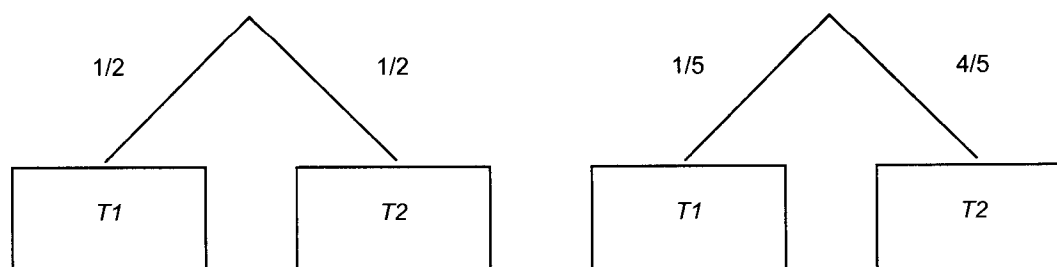


Figure 8. Threat trees for $P1$ and $P2$.

The simplest approach to construct a pair of platform trees consistent with the threats trees in Figure 8 is to assume two bits of information. First, assume the quantity of $T1$ -

type threats is known, say 100, and secondly, assume that the quantity of *T1*-type threats which engage *P1*-type platforms is also known, say 90.

Let x_{ij} denote the quantity of *Ti* threats that engage a *Pj* platform. In this instance, both *i* and *j* take values 1 or 2.

From the paragraph just after Figure 8, $x_{11} + x_{12} = 100$, that is, the total number of *T1*-type threats is 100, and $x_{11} = 90$, that is, the number of *T1*-type threats that engage *P1*-type platforms is 90. It follows that $x_{12} = 10$. In order to be consistent with the threats in Figure 8, it must be the case that $x_{21} = 90$ (equal numbers of each threat engage *P1*), and that $x_{22} = 40$ (the number of *T2*s that engage a *P2* is four times the number of *T1*s that engage a *P2*). This implies that the platform trees for this scenario are those given in Figure 9.

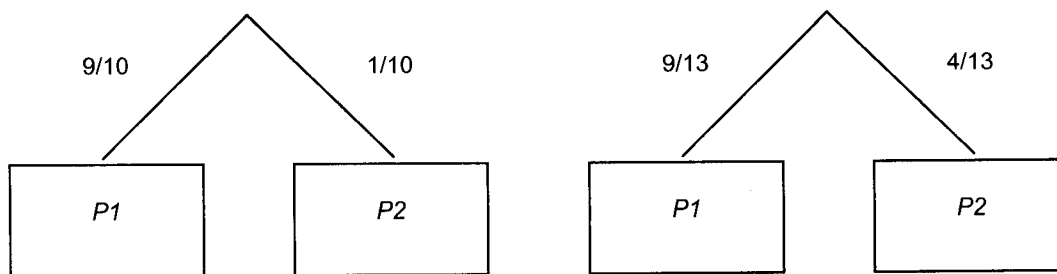


Figure 9. Platform trees for *T1* and *T2*, consistent with Figure 8.

In pursuit of a pair of platform trees distinct from those in Figure 9, but still consistent with the threat trees of Figure 8, it's only required that a different assumption regarding x_{11} be made. Thus, leave $x_{11} + x_{12} = 100$, but take $x_{11} = 50$, rather than 90 as above. Then $x_{12} = 50$. And to preserve consistency with the threat trees in Figure 8, $x_{21} = 50$, and $x_{22} = 200$. Thus, the platform trees for this scenario are those given in Figure 10.

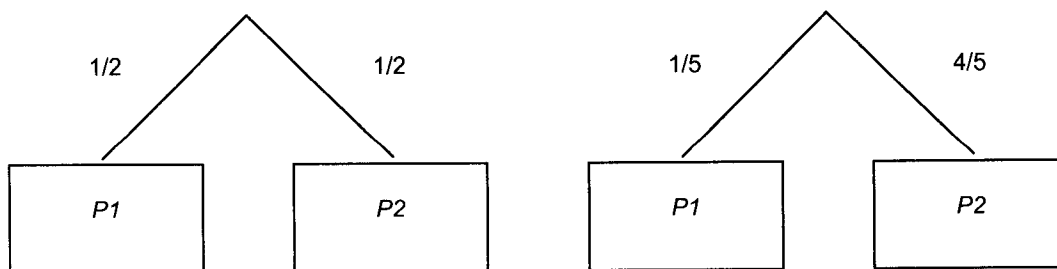


Figure 10. Platform trees for *T1* and *T2*, consistent with Figure 8.

Since the platform trees in Figures 9 and 10 are clearly distinct, and since both are consistent with the threat trees given in Figure 8, the title of this section has been established, that is, threat trees do not determine platform trees.

THREAT TREES ARE NOT DETERMINED BY PLATFORM TREES

To demonstrate that threat trees are not determined by platform trees it is sufficient to construct a pair of platform trees that are consistent with two distinct pairs of threat trees. To this end consider the platform trees given in Figure 11.

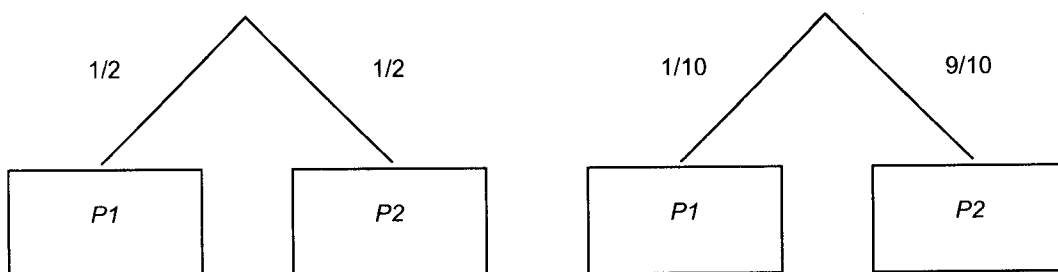


Figure 11. Platform trees for $T1$ and $T2$.

The simplest approach to construct a pair of threat trees consistent with the platform trees in Figure 11 is to assume two bits of information. First, assume the quantity of $T1$ -type threats is known, say 100, and secondly, assume that the quantity of $T2$ -type threats is also known, also say 100.

As in the preceding section, let x_{ij} denote the quantity of Ti threats that engage a Pj platform. In this instance, both i and j take values 1 or 2.

From the paragraph just after Figure 11, $x_{11} + x_{12} = 100$, that is, the total number of $T1$ -type threats is 100, and $x_{21} + x_{22} = 100$, that is, the number of $T2$ -type threats is 100. In order to be consistent with the first of the platform trees in Figure 11, it must be the case that $x_{11} = x_{12} = 50$ ($T1$ engages equal numbers of each platform type). In order to be consistent with the second platform tree in Figure 11, $x_{21} = 10$ (the number of $T2$ s that engage a $P1$ is one-tenth of the total quantity of $T2$ s), and $x_{22} = 90$ (the number of $T2$ s that engage a $P2$ is nine-tenths of the total quantity of $T2$ s). These values imply that the threat trees for this scenario are those given in Figure 12.

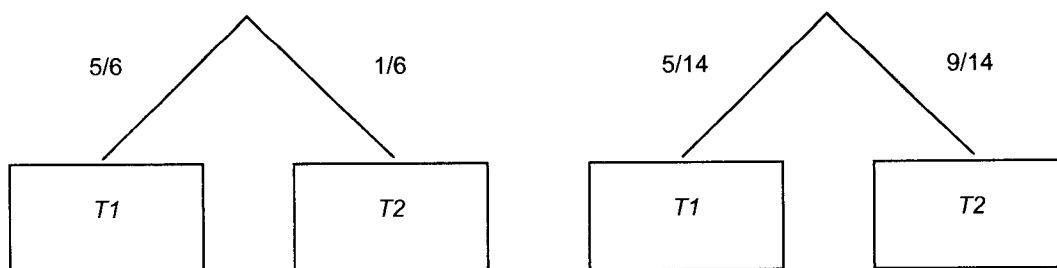


Figure 12. Threat trees for $P1$ and $P2$, consistent with Figure 11.

In pursuit of a pair of threat trees distinct from those in Figure 12, but still consistent with the platform trees of Figure 11, it's only required that a different assumption regarding the quantity of $T2$ -type threats be made. Thus, leave $x_{11} + x_{12} = 100$, but take $x_{21} + x_{22} = 300$, rather than 100 as above. Then to preserve consistency with the platform trees of Figure

11, $x_{11} = x_{12} = 50$, and $x_{21} = 30$, $x_{22} = 270$. Thus, the threat trees for this scenario are those given in Figure 13.

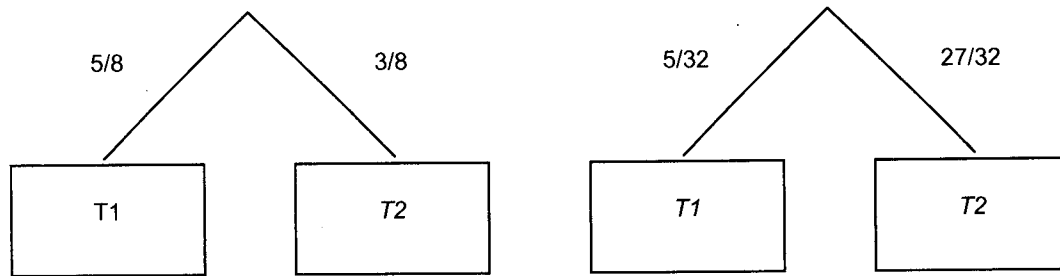


Figure 13. Threat trees for $P1$ and $P2$, consistent with Figure 11.

Since the threat trees in Figures 12 and 13 are clearly distinct, and since both are consistent with the platform trees given in Figure 11, the title of this section has been established, that is, platform trees do not determine threat trees.

REQUIRED: A QUANTITY MATRIX

Careful attention to the above examples is sufficient to determine what is in fact required in order to specify a particular battlefield scenario, and that is a *quantity matrix*, where the number of rows in the matrix equals the number of threat-types in the scenario, and the number of columns in the matrix equals the number of platform-types in the scenario, with the requirement that entry in the i th-row and j th-column of the matrix provides the quantity of T_i -type threats allocated to attach P_j -type platforms.

Furthermore, a quantity matrix for a given scenario uniquely determines the threat tree for each platform in the scenario, and also uniquely determines the platform tree for each threat in the scenario. The converse is not, however, true. In fact, a collection of threat trees and platform trees for each platform and threat, respectively, in a given scenario may not even be consistent. That is, there may be no quantity matrix they are all in agreement with. Thus, the quantity matrix itself is the fundamental data item that is required for the analyst to study a system-of-systems scenario.

CONCLUSIONS

It has been shown that neither threat trees, platform trees, or both provide the analyst with sufficient information to adequately represent a force-on-force scenario for the purpose of survivability tradeoff analysis in a system-of-systems environment, but that a quantity matrix as defined above is adequate.

It's interesting to note that both Schwarz, [2], and Hicks generally created the threat trees required of them in survivability studies by creating a quantity matrix for a single platform, and then suppressing the quantity data, leaving only the probabilities of encounter.

Thus, perhaps not surprisingly, what the analyst requires for a tradeoff analysis of a future force is an inventory of the battlefield.

BIBLIOGRAPHY

- [1] *TOSOM User's Manual.*
- [2] Frederick Schwarz, personal communication.